EURASIP Journal on Image and Video Processing

RESEARCH Open Access

Geolocation of covert communication entity on the Internet for post-steganalysis

Fan Zhang[1,2], Fenlin Liu[1,2*] and Xiangyang Luo[1,2]

Abstract

Geolocation of covert communication entity is significantly important for the forensics of the crime but has significant challenges when the steganalyst locks the guilty actor IP and wants to know the physical location of the actor. This kind of post-steganalysis involves not only the stegos transmitted on the Internet but the IP package head and content. This paper presents a geolocation method for the location of the covert communication entity based on hop-hot path coding. The method estimates the location of the covert communication entity by combining the path and delay between probes and the covert communication entity IP, which improves the deficiency that similar delays do not necessarily mean close geographical locations of the IPs. Moreover, the similarity between the IPs' paths can be measured by coding the paths between IPs and probes. The results of a series of experiments show that the median error of the proposed method is within 6.16 km using different thresholds.

Keywords: Covert communication, Entity geolocation, Post-steganalysis, Forensics

1 Introduction

Steganography embeds secret messages into unsuspicious carriers and transmits the messages through public channels for covert communication without attracting attention [1]. This kind of communication not only hides the secret messages but also the communication behavior as the carriers are accessible to anyone on the public channels. As the steganography techniques could be maliciously used for stealing confidential information, it is practically significant to carry on researches to forensics of the crime. For decades, researchers have proposed many techniques for the forensics of steganography, including the stego detection [2–10], the payload location [11–15], the embedding key restore [16, 17], the secret message extraction [17], and the steganographer detection [18–20]. In practice, the covert communication entity on the Internet usually acts as the user of social platforms, whose location is virtual. Even if the covert communication entity is successfully detected, the physical location of the covert communication entity is still unknown. To achieve the complete forensics of the crime, the post-steganalysis that investigates the physical location of the covert communication entity should be carried out.

As the transmission of the stegos on the Internet involves the IP (Internet Protocol) packages and the IP usually reflects the physical location of the client, the physical location of the covert communication entity can be located based on the IP addresses in the IP packages of the stegos. At present, street-level geolocation method is suitable for locating the covert communication entity, such as SLG (Street-Level Geolocation) method [21] IRLD (Identification Routers and Local Delay Distribution Similarity based Geolocation) method [22], and TNN method (IP Geolocation Algorithm based on Two-tiered Neural Networks) [23]. These methods are based on an important assumption that when probes measure IPs with similar geographic locations, the delays from probes to IPs are often similar. However, in actual Internet environment, IPs' locations with similar delays are not necessarily adjacent. Therefore, it is difficult to ensure the reliability of the results of these methods.

Aiming at the above problem, this paper presents a geolocation method for the location of the covert communication

* Correspondence: liufenlin@vip.sina.com
[1]PLA Strategic Support Force Information Engineering University, Zhengzhou 450001, China
[2]State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China

entity based on hop-hot path coding. It is worth noting that the geolocation of the entity is for the post-steganalysis where the stegos transmitted on the Internet are successfully and the entity IP is locked. With the knowledge of the covert communication entity IP, the proposed method firstly obtains landmarks around the covert communication entity (landmarks are not covert communication entities; they are IP addresses of known geographical locations), and use probes to measure the known landmarks to get the delay and path information from probes to landmarks. Then, the path is encoded to get the vector of delay and path, and probes are used to measure the covert communication entity to obtain the entity vector of delay and path. After that, the vector of delay and path of the landmarks whose network environment is similar to the entity is taken as the input, and the corresponding latitude and longitude of the landmarks are as the output to train the neural network. Finally, input the entity vector of delay and path neural network to geolocate the entity.

The rest of this paper is organized as follows. The existing typical entity geolocation methods are introduced in Section 2. Section 3 introduces the basic principle and main steps of the proposed method for the geolocation of the covert communication entity based on hop-hot path coding. The performance of the method is evaluated and discussed through the experiments in Section 4. Finally, Section 5 summarizes the work of this paper.

2 Related work

In this section, the existing typical network entity geolocation methods are briefly analyzed and the problems involved are pointed out.

Existing network entity geolocation methods usually attempt to describe the conversion or statistical relationship between delay and geographical location. The accuracy of most of these methods can only reach city level. Only a few methods, such as SLG and TNN, can geolocate the network entity at street-level granularity.

The SLG method [21] uses a three-tier geolocation process to locate the network entity. A schematic diagram of the geolocation process of SLG method is shown in Fig. 1. In tier 1, the method convert the delay between the probes and the network entity into geographical distance, and geolocate the entity into a coarse-grained region based on multilateration. In tier 2, the relative delay between the landmarks and the entity is converted into distance; then, the entity is geolocated into a fine-grained region via multilateration. In tier 3, the location of the landmark with the minimum relative delay of the entity is taken as the estimated location of the entity, for example, the landmark L3.

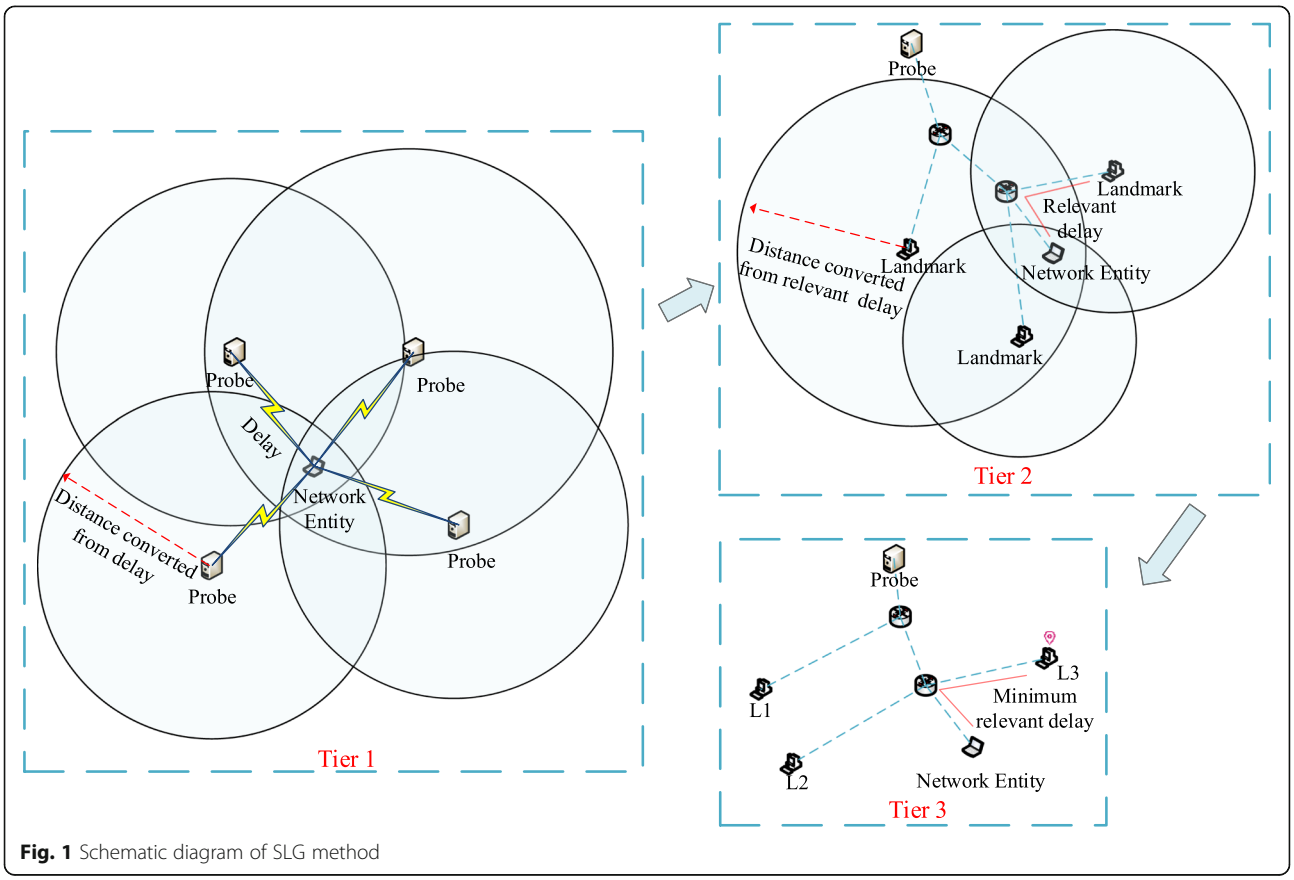

Fig. 1 Schematic diagram of SLG method

The TNN method [23] locates the network entity by training neural network; it also utilizes the idea of approaching tier by tier to geolocalize the entity. A schematic diagram of the geolocation process of TNN method is shown in Fig. 2. The method uses RBF (radial basis function) neural network and MLP (multilayer perceptron) neural network to learn the mapping between the delay and the location of the landmarks to achieve entity geolocation. The TNN method uses RBF neural network as the first tier to locate a smaller region in which the network entity resides, and then uses MLP neural network as the second tier to estimate its location more accurately within that region.

Under normal circumstances, the above methods based on delay can achieve street-level entity geolocation. However, the delays of probes measuring entity can only represent the distance between the probes and the entity. In actual network environment, due to indirect or circuitous routing, entities with similar delays may be far apart, which will cause unreliable geolocation result. In order to overcome the above problems and improve reliability in entity geolocation, an entity geolocation method based on delay and path is proposed in this paper. Different from the above typical methods, the proposed method not only estimates the location of entity by delay but also takes into account the paths between the probes and the entity.

3 The proposed method

A large amount of measurement data shows that the end-to-end distance in the Internet can be approximated by delay, and the direction is determined by the path. According to this basic fact, the geolocation method trains neural networks based on the combination of delay and path. Because of the ISPs (Internet service providers) of the covert communication entities are unknown and ISPs in some countries do not fully realize the interconnection within the city, when geolocating the covert communication entities, we need to use landmarks around the entities to ensure the consistency of training samples.

The method is divided into six parts: obtaining landmarks, vectors construction of landmarks, acquisition of training sets, training neural networks, vector construction of the covert communication entity, and entity geolocation. Figure 3 shows the frame diagram of the method.

The specific steps of the method are as follows:

1) *Obtaining landmarks*. With the knowledge of the covert communication entity IP, get landmarks around the entity.
2) *Vector construction of landmarks*. Deploying n probes $P_1, P_2, \ldots, P_n$, acquiring the delay and path from the probes to landmarks. Then, encoding the path with hop-hot path code method to get the vectors of delay and path

$$V_k = \left(d_{k,1}, d_{k,2}, \ldots, d_{k,n}, C_k\right). \tag{1}$$

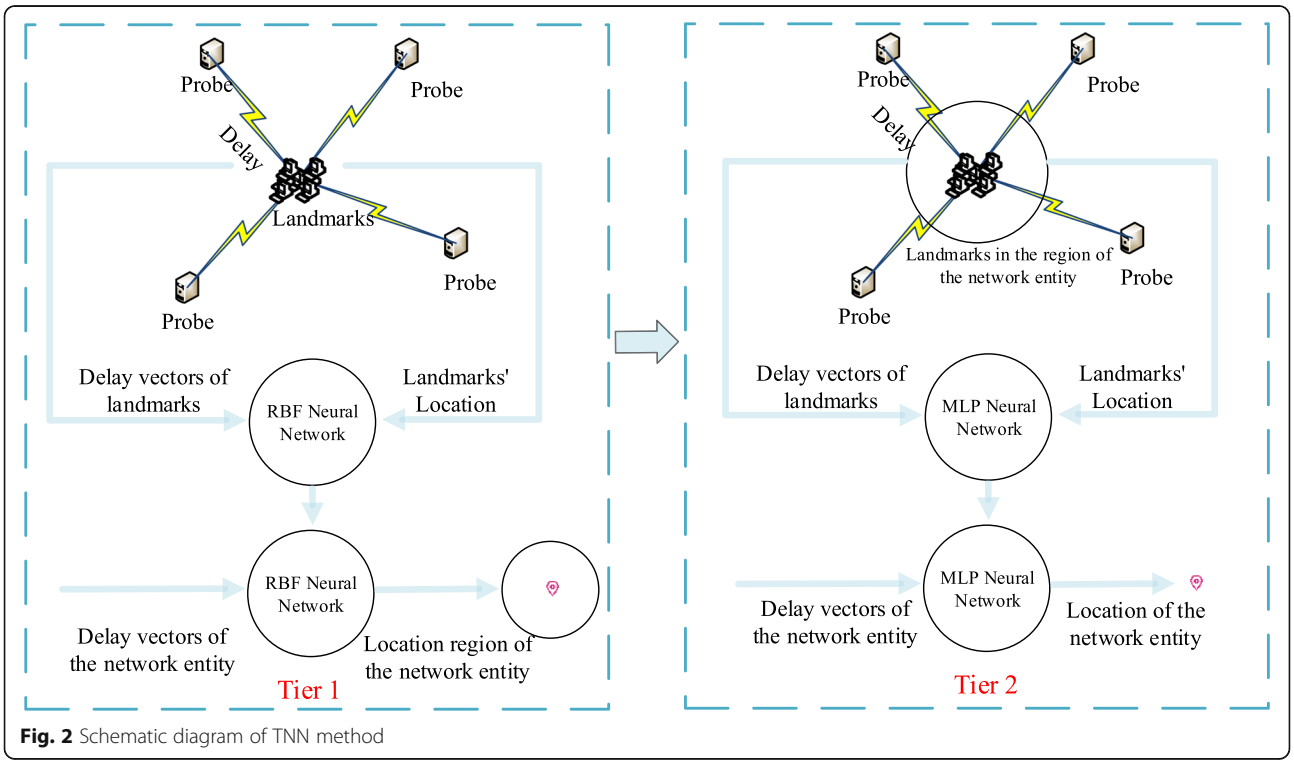

Fig. 2 Schematic diagram of TNN method

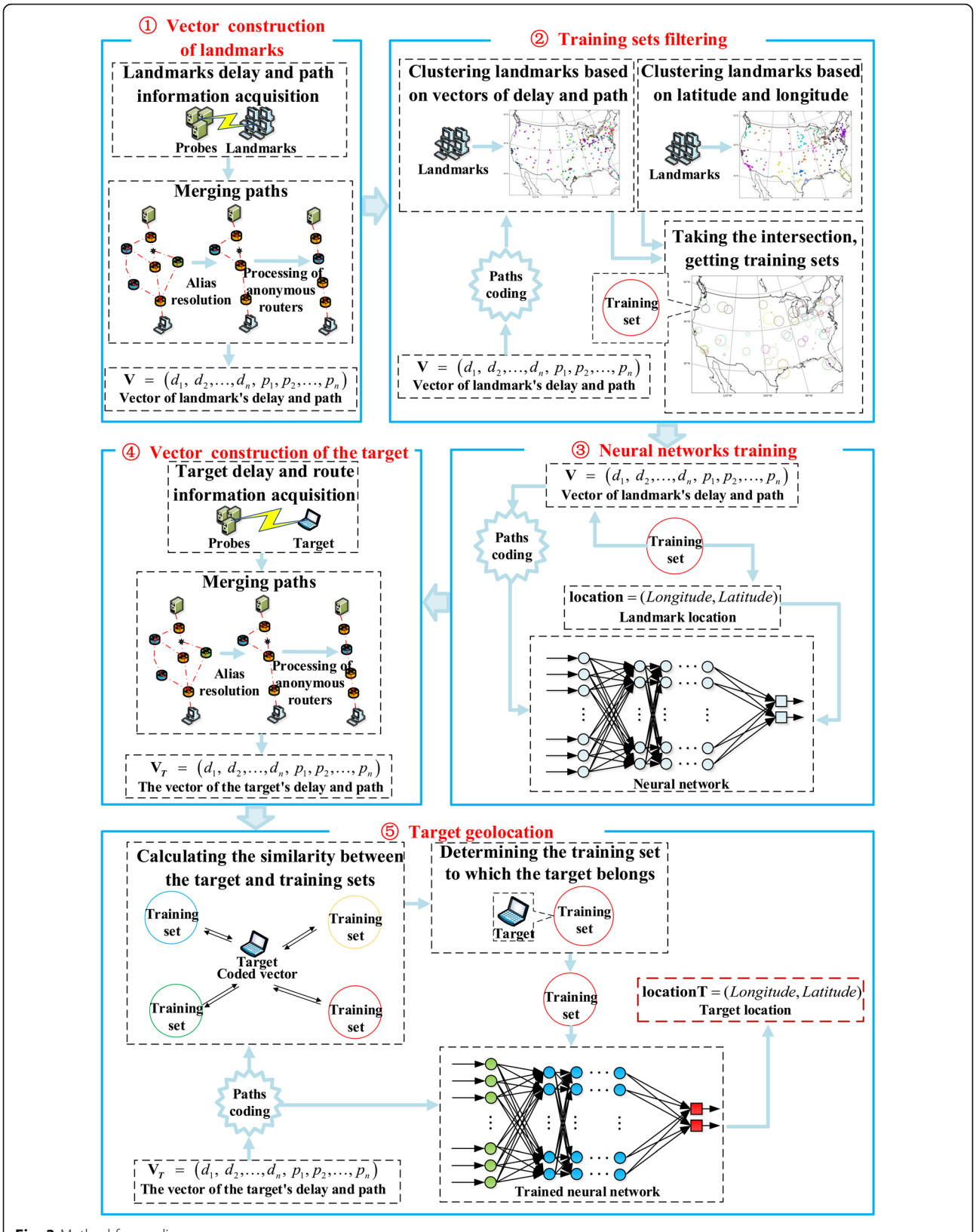

Fig. 3 Method frame diagram

where V_k represents the vector of delay and path of the k th landmark, and $d_{k,\ i}$ represents the delay from the probe i to the landmark k. C_k represents the encoded path vector of the landmark k.*Acquisition of training sets*. Use (1) to cluster the landmarks, and then use the latitude and longitude of the landmarks to cluster the landmarks. Take the intersection of the two clustering results to obtain the training sets, denoted as

$$F = \{S_1, S_2, ..., S_q\}. \tag{2}$$

where S_i is the i th training set.

3) *Neural networks training*. Train the neural network for each training set. Taking (1) in the training set S_i as input, and the latitude and longitude thereof as output, obtaining a well-trained neural network.
4) *Vector construction of the covert communication entity*. Acquiring the delay and path from the probes to entity. Encoding the path to get the vector of delay and path of the covert communication entity

$$V_T = (d_1, d_2, ..., d_n, C_T). \tag{3}$$

where V_T represents the vector of delay and path of the covert communication entity, and d_i represents the delay from the probe i to the entity. C_T represents the encoded path vector of the entity.

5) *Geolocation of covert communication entity*. Calculate the similarity sim_i from (3) to S_i.Setting the threshold U, and let $M = \max_{i=1,...,q}(sim_i)$, if $M \geq U$, inputting (3) into the neural network constructed by S_i to obtain its latitude and longitude; otherwise, ending the method.

Among them, hop-hot path coding method, acquisition of training sets, and geolocation of covert communication entity are the important parts of the method, which will be described in detail in the following subsections.

3.1 Hop-hot path coding method

The path from probe to the entity IP is composed of router sequence, such as <probe, router$_1$, router$_2$, ..., router$_n$, entity IP>. One-hot coding can be used to measure the similarity between paths by judging whether routers in the paths, but the paths are sequential, one-hot coding cannot express this sequential well, so it is not very reasonable to express the paths by one-hot encoding. In order to better measure the degree of similarity between paths, this paper proposes a path coding method: hop-hot path coding. It can make the coded path vector directly into the machine learning model as a feature or compare similarity.

The process of coding is as follows. Firstly, stable router paths are obtained from probes to all landmarks, and all router sets are obtained. Then, the one-hot coding is used to encode each stable router path to obtain the path vector. After that, the path vector is quantized by hop number. Finally, the entity's router path vector is quantized. The details are as follows:

Step 1. *Building router path set*. n probes are used to measure m landmarks, then, a stable router path set whose size is $n \times m$ obtained. The set is recorded as

$$\mathbf{E} = \begin{Bmatrix} p_{1,1}, p_{1,2}, ..., p_{1,n} \\ p_{2,1}, p_{2,2}, ..., p_{2,n} \\ ... \\ p_{m,1}, p_{m,2}, ..., p_{m,n} \end{Bmatrix}. \tag{4}$$

where $p_{k,\ i}$ is the measured router path from the *ith* probe to the *kth* landmark.

Step 2. *Extracting routers*. All routers in the router paths from the *ith* probe to m landmarks are extracted. The extracting result is

$$\mathbf{O}_i = \{r_{i,1}, r_{i,2}, ..., r_{i,l_i}\}. \tag{5}$$

where $r_{i,\ j}$ is the *jth* router in the measured paths from the *ith* probe to m landmarks, and the order is inessential. l_i is the number of routers appearing in the measured paths whose source is the *ith* probe. The feature space of path coding is consistent to all $\mathbf{O}_i$, and the feature space is recorded as

$$\mathbf{L} = \{\mathbf{O_1}, \mathbf{O_2}, ..., \mathbf{O_n}\}. \tag{6}$$

That is equivalent to

$$\mathbf{L} = \{\{r_{1,1}, r_{1,2}, ..., r_{1,l_1}\}, \{r_{2,1}, r_{2,2}, ..., r_{2,l_2}\}, ..., \{r_{n,1}, r_{n,2}, ..., r_{n,l_n}\}\}. \tag{7}$$

where n is the number of probes.

Step 3. *Building landmarks' router path vector*. For landmark k, according to the router paths from each probe to landmark k, the landmark is coded in feature space $\mathbf{L}$. The coding result is recorded as

$$\mathbf{C_k} = (V_{1,1,k}, V_{i,j,k}, ..., V_{n,l_n,k}). \tag{8}$$

The value of $V_{i,\ j,\ k}$ is donated as

$$V_{i,j,k} = \begin{cases} \beta, & if\ r_{i,j}\ not\ in\ p_{i,k} \\ H_{i,j,k}, & if\ r_{i,j}\ in\ p_{i,k} \end{cases} \tag{9}$$

where $H_{i,\ j,\ k}$ is the number of hops from the router $r_{i,\ j}$ to landmark k, and β is a control parameter whose value is greater than the length of $p_{x,\ y}$, $(1 \leq x \leq m, 1 \leq y \leq n)$.Step 4. Building the router path vector of the covert

communication entity. As the same of landmark, the coding result of entity in feature space L is recorded as

$$\mathbf{C}_T = \left(V_{1,1,T}, V_{i,j,T}, ..., V_{n,l_n,T} \right). \tag{10}$$

The value of $V_{i,\,j,\,T}$ is donated as

$$V_{i,j,T} = \begin{cases} \beta & if\ r_j\ not\ in\ p_{i,T} \\ H_{i,j,T} & if\ r_j\ in\ p_{i,T} \end{cases} \tag{11}$$

where $H_{i,\,j,\,T}$ is the number of hops from the router $r_{i,\,j}$ to entity T. Meanwhile, if a router is in the router path from probes to entity but not in the router paths from probes to the landmarks, this router would not be considered.

3.2 Acquisition of training sets

In the actual Internet environment, there are multiple ISPs in some countries and regions. Even if the landmarks' locations are close, there may also be large gaps in vectors of delay and path between landmarks. If all the landmarks are used as the training set to train the neural network, the mapping relationship learned by it will not be strong, and the geolocation reliability is hard to guarantee. Therefore, the training set needs to be filtered so that the delays, paths, latitude, and longitude of the landmarks in each training set are similar. The specific steps are as follows:

Input: Vectors of delay and path of landmarks, longitude, and latitude of landmarks

Output: Filtered training sets

Step 1. Using (1) to perform K means clustering on the landmarks, wherein k value is iterated from small to big, calculating the contour coefficients of the clustering, selecting the k value corresponding to the maximum contour coefficient, recording the clustering set as $\mathbf{K} = \{D_1, D_2, ..., D_k\}$.Step 2. Using the latitude and longitude in the landmark set to cluster all the landmarks, in terms of the number of clusters, also selecting the value corresponding to the maximum contour coefficient and recording it as h, and recording the clustering set as $\mathbf{Q} = \{L_1, L_2, ..., L_h\}$.Step 3. Calculating $\mathbf{F} = \mathbf{K} \cap \mathbf{Q}$ and recording the final set of categories as $\mathbf{F} = \{S_1, S_2, ..., S_q\}$.At this time, the delay, path, latitude, and longitude of the landmarks in each training set are similar. The neural network is trained by using the landmarks in each training set, and the mapping between delay, path, and location will be more reliable.

Table 1 Experimental setups

Landmark deployment	New York State	2384
	Chinese Mainland	11286
	Hong Kong	39763
Probe deployment	China: four probes deployed, in Beijing, Chengdu, Shanghai and Wuhan, respectively.	
	The United States: five probes deployed in Washington, Silicon Valley, New York, Atlanta, and Seattle, respectively.	
Detection protocol	ICMP-PARIS [24]	

Table 2 Statistics of stable path ratio

Training set size	The quantity of categories in the region		
	Chinese Mainland	Hong Kong	New York State
Training set size > 100	28	9	3
Training set size > 300	5	7	2
Training set size > 500	2	6	2

3.3 Geolocation of covert communication entity

After training the neural network for each training set, when geolocating the covert communication entity, it is first necessary to judge the training set to which the entity belongs. Then, the vector of delay and path is input into the neural network trained by the training set to obtain the latitude and longitude of the entity. Specific steps are as follows:

Input: The vector of delay and path of the entity

Output: Longitude and latitude of the entity

Step 1. Calculate the cosine similarity between the center of D_i and (3), and choose the D_i with the highest cosine similarity between center and (3) as the D_i to which the entity T belongs.

Step 2. Calculate the cosine similarity between landmarks in D_i and the entity. Find the landmark whose vector of delay and path is most similar to the entities' vector. Record the training set to which the landmark belongs as S_j, and use S_j as the training set of the entity. The vector similarity between landmark and entity is

Table 3 Relationship between different training set sizes, different thresholds and the quantity of the entities that can be geolocated and geolocation error

Landmark sets	$U^{\bigstar}$	QCG/QCNG$^{\bullet}$	MGE$^{\blacklozenge}$
Training set size[§] > 100 (a total of 40 training sets and 41,231 landmarks)	0.9	9321/1365	2.80 km
	0.8	10109/577	4.62 km
	0.7	10549/137	6.16 km
Training set size > 300 (a total of 14 training sets and 37,134 landmarks)	0.9	8203/2483	2.26 km
	0.8	8748/1938	2.97 km
	0.7	9108/1578	4.05 km
Training set size > 500 (a total of 10 training sets and 32,241 landmarks)	0.9	7296/3390	2.18 km
	0.8	8052/2634	2.51 km
	0.7	8724/1962	2.96 km

[§]"Training set size > N" represents a landmark set composed of all training sets with a landmark quantity greater than N in the training set

$^{\bigstar}U$ is short for "geolocation threshold"

$^{\bullet}$QCG is short for "quantity of the entities that can be geolocated"
QCNG is short for "quantity of the entities that cannot be geolocated"

$^{\blacklozenge}$MGE is short for "median geolocation error of the entities that can be geolocated"

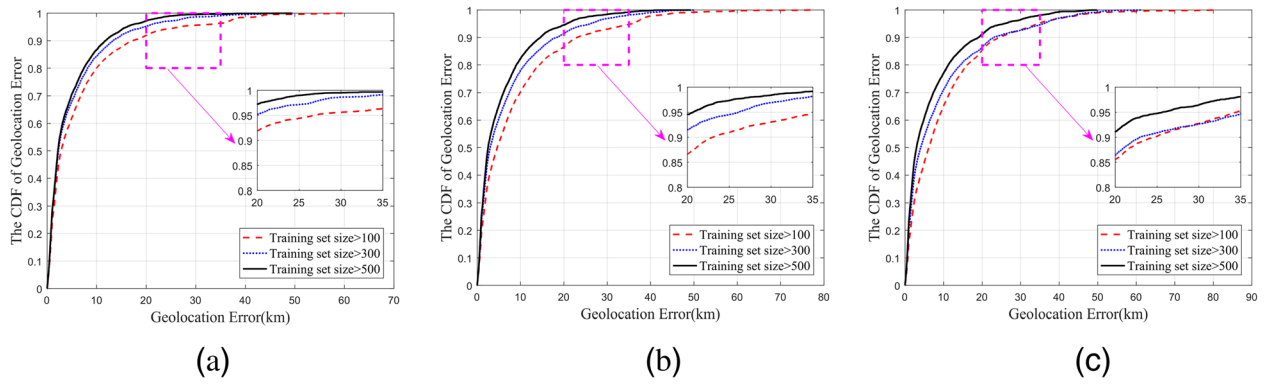

Fig. 4 The CDF (cumulative distribution function) of geolocation error under different training set sizes and thresholds. The red dashed line, blue dot line, and the black solid line indicate the cumulative error distribution of all neural networks formed by the training sets with the landmarks greater than 100,300 and 500 in each training set for the corresponding entities geolocation, respectively. **a** Threshold is 0.9. **b** Threshold is 0.8. **c** Threshold is 0.7

recorded as M.Step 3. Setting the threshold U, and if $M \geq U$, using the neural network formed by the training set S_j to geolocate the entity; otherwise, ending the method.

4 Experimental results and discussion

This paper focuses at the geolocation of the covert communication entity on the Internet with the knowledge of the entity IP, while the detection of the stegos on the Internet and the acquisition of the IP address from the stegos IP packages are beyond this paper. In this section, the rationality and effectiveness of the proposed method are verified by two experiments: verification on the geolocation effect of the method, and comparative verification. The experimental setups are shown in Table 1.

In this paper, 53,433 measurable street-level landmarks in Chinese Mainland, New York State (USA), and Hong Kong (China) have been measured for 14 days and 3000 times with nine probes located in Beijing, Chengdu, Shanghai, Wuhan, Washington, Silicon Valley, New York, Atlanta, and Seattle. A large amount of path and delay information has been obtained.

The path acquisition part of the method combines the method of merging router aliases such as Ally, Mercator [25, 26], and the anonymous route parsing method in [27]. Merge the routers in the path from each probe to the landmark and select the most frequently occurring path as the path information, then set β to 30 empirically when encoding the path.

In order to obtain more accurate delay information, during network measurement, the delay from the probes to the landmarks is repeatedly measured, and the minimum delay on the stable path is selected as the delay information. The delay information on the stable path often represents the network stability and less congestion. Therefore, the obtained delay information is closer to the true propagation delay.

When training neural networks, MLP neural networks [28] are used, with formula (1) as the input of the neural networks, and the latitude and longitude of the landmark as the output of the neural networks. A neural network is trained for each training set.

Table 4 The proportion of geolocation error when the threshold is 0.9

Training set size	Geolocation method	PGE < 10 km▲	PGE < 20 km	PGE < 40 km
> 100	Proposed method	80.1%	91.9%	98.5%
	SLG method [21]	60.5%	83.6%	94.1%
	TNN method [23]	37.2%	83.7%	94.9%
> 300	Proposed method	84.3%	95.2%	99.5%
	SLG method [21]	55.4%	79.7%	90.1%
	TNN method [23]	35.7%	81.4%	94.2%
> 500	Proposed method	86.7%	97.2%	99.9%
	SLG method [21]	58.0%	81.7%	91.2%
	TNN method [23]	34.4%	78.5%	94.7%

▲"PGE < X" is short for "proportion of the entities within geolocation error being X".

The experimental results show that the proposed method can achieve street-level geolocation for the given IP of covert communication entity. Compared with the existing typical geolocation methods, the proposed method improves the deficiency that similar delays do not necessarily mean close geographical locations of the IPs, thereby improving geolocation accuracy. This is because the existing typical methods only rely on the delay for geolocation, while the delay in the network only has the significance of distance. The similar delays do not necessarily mean close geographical locations of the IPs, because their measurement paths may be completely different, which makes the existing typical methods less reliable. The proposed method combines the distance meaning of delay and the direction meaning of path to estimate the location of the entity. The entities with similar delay and path must have similar geographical location, so as to solve the above problem and improve the reliability of location

4.1 Experiment of entity geolocation with different parameters

Based on the experimental setups in Table 1, we verify the effect of the geolocation method for the location of the covert communication entity in this subsection. To verify the geolocation error, 80% of the landmarks are randomly selected from each region as the candidate set of the training set for training network, and the remaining 20% of the landmarks (a total of 10,686) are used as the covert communication entities for geolocation verification. The landmarks can be divided into 145 categories by using the landmarks clustering in the method. Table 2 shows the relationship between the size of the training set, the number of clusters and the geographical location thereof.

Table 3 shows the geolocation effects of training sets in different training sizes and different geolocation thresholds on the corresponding entities.

Figure 4 shows the geolocation error cumulative distribution of the entities that can be geolocated under different training set sizes and different threshold conditions.

Table 3 and Fig. 4 show that as the training scale N increases, the number of samples in a single training set is

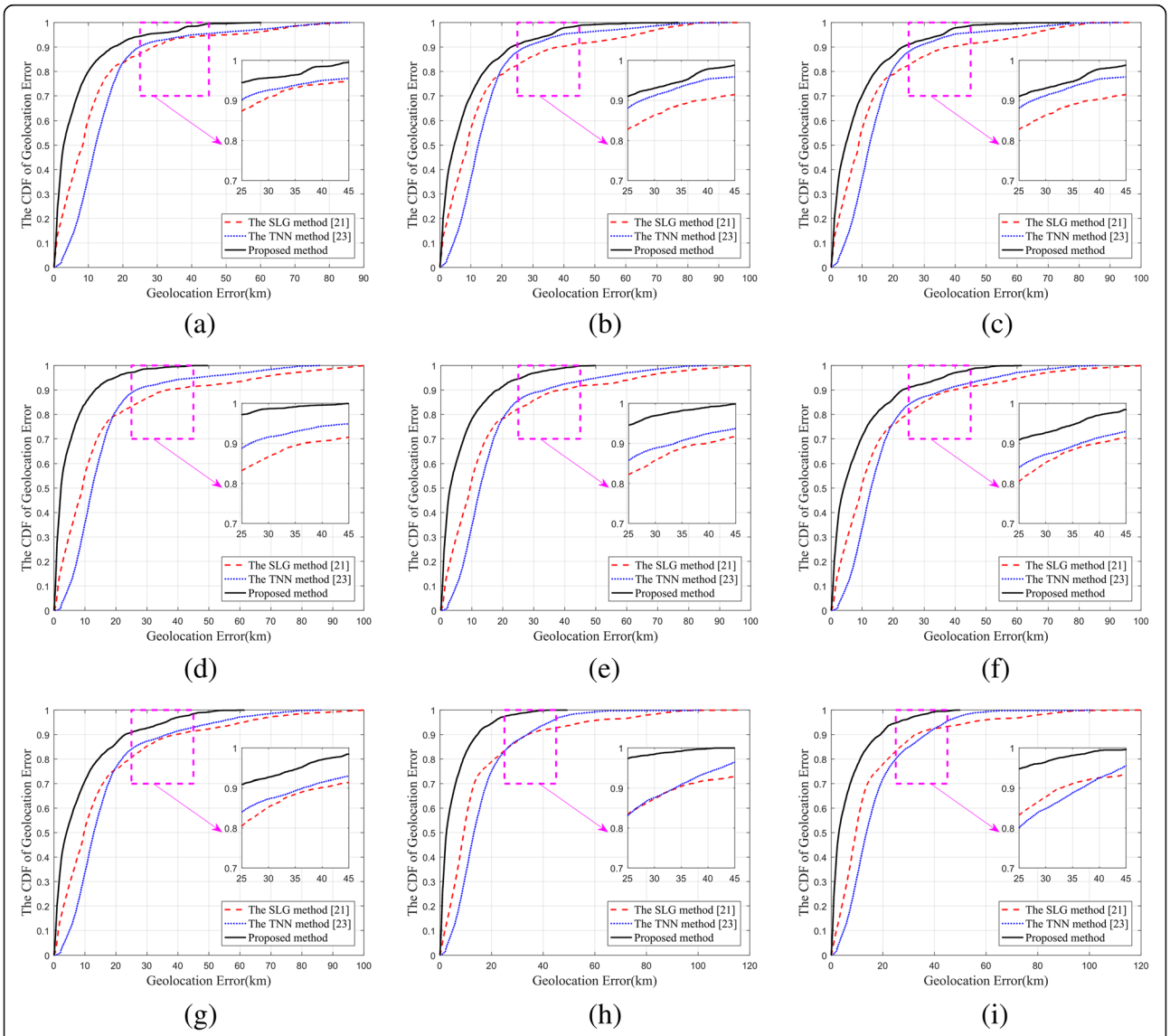

Fig. 5 Comparison on IP geolocation error under the same conditions. The black line, red dashed line, and blue dot line indicate the geolocation error cumulative distribution of the proposed method, SLG method, and TNN method, respectively. **a** The training set size > 100, and the threshold is 0.9. **b** The training set size > 100, and the threshold is 0.8. **c** The training set size > 100, and the threshold is 0.7. **d** The training set size > 300, and the threshold is 0.9. **e** The training set size > 300, and the threshold is 0.8. **f** The training set size > 300, and the threshold is 0.7. **g** The training set size > 500, and the threshold is 0.9. **h** The training set size > 500, and the threshold is 0.8. **i** The training set size > 500, and the threshold is 0.7

increasing, but the total number of landmarks in the landmark set is decreasing, the number of locatable entities is also decreasing, and the geolocation error is decreasing. The reason is that the network trained by the training set that does not satisfy a certain sample number is not universal, which is statistically reasonable. It can also be seen that different geolocation thresholds have different degrees of impact on the number of localizable entities and geolocation error. From the experimental results, this method has certain advantages in street-level geolocation.

4.2 Comparative verification

In this subsection, we compare the geolocation effect of the proposed method with the typical geolocation methods under the situations of same entities and landmarks. Table 4 shows the statistical results of proposed method, SLG method, and TNN method when the geolocation threshold is 0.9, and the geolocation error is 10 km, 20 km, and 40 km. Fig. 5 shows the geolocation cumulative distribution of the proposed method in this paper, the SLG method and the TNN method.

As can be seen from Table 4 and Fig. 5, the reliability of the street-level positioning method of this method at 10 km, 20 km, and 40 km is better than the existing typical street-level methods.

5 Conclusions

Traditional steganalysis mainly detect whether the investigated object carries secret messages, while a few works are reported for the payload location, the embedding key restore, the secret message extraction and the steganographer detection. The geolocation of the covert communication entity reveals the physical location of the steganography on the Internet based on the IP address in the IP packages of the stegos. This paper presents a method for the geolocation of the covert communication entity based on hop-hot path coding. We do a preliminary work on the geolocation of the covert communication entity and there are still some geolocation errors as it is difficult to locate the covert communication entity within the last kilometer. Nevertheless, our method is very helpful to geolocate the covert communication entity in a certain area, and the geolocation accuracy is improved compared with the existing geolocation methods. In addition, the hop-hot path coding method in this paper is just an attempt. Whether there is a better coding method that is worth further exploring.

Abbreviations

U: Geolocation threshold; QCG: Quantity of the entities that can be geolocated; QCNG: Quantity of the entities that cannot be geolocated; MGE: Median geolocation error of the entities that can be geolocated; PGE < X: Proportion of the entities within geolocation error being X

Acknowledgements

Not applicable.

Authors' contributions

FZ and FL conceived the idea. XL designed the experiments. FZ performed the experiments. FZ, FL wrote the paper. All authors read and approved the final paper.

Funding

This work was supported by the National Natural Science Foundation of China (no.U1636219, 61602508, 61772549, U1736214, U1804263), the National Key R&D Program of China (no. 2016YFB0801303, 2016QY01W0105), and the Science and Technology Innovation Talent Project of Henan Province (no. 184200510018).

Availability of data and materials

The datasets used and analyzed during the current study are available from the corresponding author on reasonable request.

Competing interests

The authors declare that they have no competing interests.

Received: 11 December 2019 Accepted: 13 March 2020
Published online: 06 April 2020

References

1. W. Tang, B. Li, S. Tan, M. Barni, J. Huang, CNN-based adversarial embedding for image steganography. IEEE Trans. Inf. Forensic Secur. **14**(8), 2074–2087 (2019)
2. Y. Ma, X. Luo, X. Li, Z. Bao, Y. Zhang, Selection of rich model steganalysis features based on decision rough set α-positive region reduction. IEEE Trans. Circuits Syst. Video Technol. **29**(2), 336–350 (2019)
3. M. Boroumand, M. Chen, J. Fridrich, Deep residual network for steganalysis of digital images. IEEE Trans. Inf. Forensic Secur. **14**(5), 1181–1193 (2019)
4. J. Ye, J. Ni, Y. Yi, Deep learning hierarchical representations for image steganalysis. IEEE Trans. Inf. Forensic Secur. **12**(11), 2545–2557 (2017)
5. R. Zhang, F. Zhu, J. Liu, G. Liu, Depth-wise separable convolutions and multi-level pooling for an efficient spatial CNN-based steganalysis. IEEE Trans. Inf. Forensic Secur (2019). https://doi.org/10.1109/TIFS.2019.2936913
6. J. Fridrich, J. Kodovsky, Rich models for steganalysis of digital images. IEEE Trans. Inf. Forensic Secur. **7**(3), 868–882 (2012)
7. B. Li, Z. Li, S. Zhou, S. Tan, X. Zhang, New steganalytic features for spatial image steganography based on derivative filters and threshold LBP operator. IEEE Trans. Inf. Forensic Secur. **13**(5), 1242–1257 (2018)
8. P. Wang, F. Liu, C. Yang, Towards feature representation for steganalysis of spatial steganography. Signal Process. (2019). https://doi.org/10.1016/j.sigpro.2019.107422
9. C Yang, Y Zhang, P Wang, X Luo, F Liu, J Lu, Steganalysis feature subspace selection based on fisher criterion. IEEE International Conference on Data Science and Advanced Analytics, Tokyo, Japan, 19-21 October 2017.
10. L. Xiang, G. Guo, J. Yu, V.S. Sheng, P. Yang, A convolutional neural network-based linguistic steganalysis for synonym substitution steganography. Math. Biosci. Eng. **17**(2), 1041–1058 (2019)
11. T.T. Quach, Optimal cover estimation methods and steganographic payload location. IEEE Trans. Inf. Forensic Secur. **6**(4), 1214–1222 (2011)
12. J. Liu, Y. Tian, T. Han, C.F. Yang, W.B. Liu, LSB steganographic payload location for JPEG-decompressed images. Digit. Signal Prog. **38**, 66–76 (2015)
13. Y. Sun, H. Zhang, T. Zhang, R. Wang, Deep neural networks for efficient steganographic payload location. J. Real-Time Image Process. **16**(3), 635–647 (2019)
14. C. Yang, F. Liu, S. Ge, J. Lu, J. Huang, Locating secret messages based on quantitative steganalysis. Math. Biosci. Eng. **16**(5), 4908–4922 (2019)
15. C. Yang, J. Wang, C. Lin, H. Chen, W. Wang, Locating steganalysis of LSB matching based on spatial and wavelet filter fusion. CMC-Comput. Mat. Contin. **60**(2), 633–644 (2019)
16. J Liu, Y Tian, T Han, J Wang, X Luo, Stego key searching for LSB steganography on JPEG decompressed image. Sci. China-Inf. Sci. 59, 32105: 1-32105:15 (2016)
17. C Yang, X Luo, J Lu, F Liu, Extracting hidden messages of MLSB steganography based on optimal stego subset. Sci. China-Inf. Sci. 61(11), 119103:1-119103:3 (2018)

18. AD Ker, T Pevný, Identifying a steganographer in realistic and heterogeneous data sets. Paper presented at Media Watermarking, Security, and Forensics, Burlingame, California, 13 February 2012.
19. M Zheng, S Zhong, S Wu, J Jiang, Steganographer detection via deep residual network. Paper presented at 2017 IEEE International Conference on Multimedia and Expo, ICME 2017, Hong Kong, China, 10-14 July 2017.
20. A.D. Ker, T. Pevný, The steganographer is the outlier: realistic large-scale steganalysis. IEEE Trans. Inf. Forensic Secur. **9**(9), 1424–1435 (2014)
21. Y Wang, D Burgener, M Flores, A Kuzmanovic, C Huang, Towards street-level client-independent IP geolocation. In Proceedings of the 8th USENIX conference on Networked systems design and implementation, Boston, MA, USA, 30 March 2011.
22. F Zhao, X Luo, Y Gan, S Zu, Q Cheng, F Liu, IP Geolocation based on identification routers and local delay distribution similarity. Concurr. Comput.-Pract. Exp. (2018). doi: https://doi.org/10.1002/cpe.4722.
23. H Jiang, Y Liu, JN Matthews, IP geolocation estimation using neural networks with stable landmarks, In 2016 IEEE Conference on Computer Communications Workshops, San Francisco, CA, USA, 10-14 April 2016.
24. B Augustin, X Cuvellier, B Orgogozo, F Viger, T Friedman, M Latapy, C Magnien, R Teixeira, Avoiding traceroute anomalies with Paris traceroute, In Proceedings of the 6th ACM SIGCOMM conference on Internet measurement, Rio de Janeriro, Brazil, 25–27 October 2006.
25. N. Spring, R. Mahajan, D. Wetherall, Measuring ISP topologies with Rocketfuel. ACM SIGCOMM Comp. Commun. Rev. **32**, 133–145 (2002)
26. R Govindan, H Tangmunarunkit, Heuristics for Internet map discovery, In Proceedings IEEE INFOCOM 2000, Conference on Computer Communications, Tel Aviv, Israel, Israel, 26-30 March 2000.
27. MH Gunes, K Sarac, Resolving anonymous routers in internet topology measurement studies, In IEEE INFOCOM 2008-The 27th Conference on Computer Communications, Phoenix, AZ, USA, 13-18 April 2008.
28. R.P. Lippmann, Pattern classification using neural networks. IEEE Commun. Mag. **27**, 47–50 (1989)

Publisher's Note